UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/403,689	10/22/1999	BERND KOWALSKI	2345/97	7576

26646 7590 03/21/2005

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
STULBERGER, CAS P	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/403,689	KOWALSKI ET AL.	
	Examiner	Art Unit	
	Cas Stulberger	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 10/22/1999; IDS filed 12/27/2004.

2. Claims 1-7 were cancelled. Claims 8-18 are pending in the case. Claims 8, 15, and 18 are independent claims.

Response to Amendment

3. Applicant's IDS filed 12/27/2004 has been considered. The grounds of rejection as set forth in the previous office action is reproduced below.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 8-11, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,425,103 to Shaw, and further in view of U.S. Patent No. 5,142,578 to Matyas et al.

In regards to claims 8 and 18, Shaw discloses the user key may be input to the present invention directly in binary form or any other suitable form (Shaw: Abstract). If the base key is longer than the user key then the user key is duplicated and the copies are appended to one another. For example, if the base key (Vernam Key) has a length of 160 bits, a user key (secret key) having a length of 48 bits must be duplicated three times (n) (Shaw: column 7, lines 60-68).

This meets the limitation of "the secret key having a defined key length, the variable parameter having a length which is a function of the defined key length." Shaw however does not disclose "communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher."

Matyas et al. discloses that public key systems are bases on dispensing with the secret key distribution channel, as long as the channel has a sufficient level of integrity (Matyas: column 2, lines 27-29). Matyas also discloses the symmetric algorithm Data Encryption Algorithm (DEA) (Matyas: column 2, lines 66-68). To transfer the DEA key over the secure channel it is encrypted with the private key and then sent to the recipient where it is decrypted with the public key (Matyas: column 3, lines 1-27). This meets the limitation of "communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher."

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of key creation as disclosed by Shaw with the method of key distribution as disclosed by Matyas in order to improve the integrity of a key distribution process (Matyas: Abstract).

6. In regards to claims 9-11, Shaw discloses combining the manipulated keys using an exclusive-OR operation (Shaw: Abstract, second sentence).

7. Claims 12-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,425,103 to Shaw, in view of U.S. Patent No. 5,142,578 to Matyas et al as applied to claim 8 above, and further in view of U.S. Patent No. 5,513,261 to Maher.

Shaw however does not disclose a PCMCIA or chipcard which stores the Vernam Key.

Maher discloses a PCMCIA card on which a user might have keys coded (column 1, lines 31-33). This meets the limitations of "the storage for the Vernam key are installed in a crypto-module separate from the encryptor, in the form of a chipcard, a multifunctional PC interface adapter, or module (PCMCIA) and only the Vernam cipher operations are performed in the encryptor."

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of key distribution and creation as disclosed by Shaw with the method of storing the key on the PCMCIA card as disclosed by Maher in order to preclude the discovery of the security parameters by unauthorized parties (Maher: Abstract).

Conclusion

8. All claims are drawn to the same invention claimed in the application prior to the entry of the submission under 37 CFR 1.114 and could have been finally rejected on the grounds and art of record in the next Office action if they had been entered in the application prior to entry under 37 CFR 1.114. Accordingly, **THIS ACTION IS MADE FINAL** even though it is a first action

after the filing of a request for continued examination and the submission under 37 CFR 1.114. See MPEP § 706.07(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cas Stulberger whose telephone number is (571) 272-3810. The examiner can normally be reached on Monday - Friday, 9:00A.M. - 6:00P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3810. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CS

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100